

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-312052

(43)Date of publication of application : 25.10.2002

(51)Int.Cl.

G06F 1/00

G06F 12/14

(21)Application number : 2001-116025

(71)Applicant : NIPPON TELEGRAPH &
TELEPHONE WEST CORP

(22)Date of filing : 13.04.2001

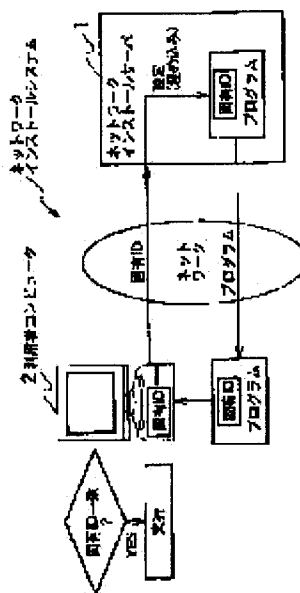
(72)Inventor : YOSHIURA AKIHIKO
IWAKIRI TAKAAKI
SAIKAWA SEIJI
TOKUSA YUKINOBU
INOUE ETSUJI
MIZUMOTO TERUAKI
WATANABE SHUICHIRO
UENO MAYUMI

(54) COMPUTER PROGRAM, ITS GENERATING METHOD, AND PROVIDING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent a computer program from being copied illegally.

SOLUTION: A network install server 1 embeds a physical address, etc., of a specific file acquired from a user computer 2 in the computer program as a proper ID and provides it to the user computer 2. This program reads the proper ID from the user computer 2 and executes the program body only when it is identical to the proper ID embedded.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-312052
(P2002-312052A)

(43) 公開日 平成14年10月25日 (2002. 10. 25)

(51) Int.Cl. ⁷	識別記号	F I	ターミナル* (参考)
G 0 6 F 1/00		G 0 6 F 12/14	3 1 0 H 5 B 0 1 7
12/14	3 1 0		3 2 0 E 5 B 0 7 6
	3 2 0	9/06	6 6 0 F

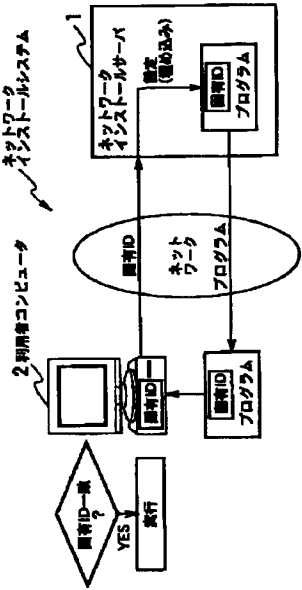
審査請求 未請求 請求項の数7 O L (全 14 頁)

(21) 出願番号	特願2001-116025(P2001-116025)	(71) 出願人	399041158 西日本電信電話株式会社 大阪府大阪市中央区馬場町3番15号
(22) 出願日	平成13年4月13日(2001. 4. 13)	(72) 発明者	吉浦 昭彦 大阪府大阪市中央区馬場町3番15号 西日本電信電話株式会社内
		(72) 発明者	岩切 高明 大阪府大阪市中央区馬場町3番15号 西日本電信電話株式会社内
		(74) 代理人	100083806 弁理士 三好 秀和 (外4名)

最終頁に続く

(54) 【発明の名称】 コンピュータプログラム、コンピュータプログラムの生成方法、コンピュータプログラムの提供方法

(57) 【要約】
【課題】 コンピュータプログラムの不正コピーを防止する。
【解決手段】 ネットワークインストールサーバ1は、利用者コンピュータ2から取得した特定ファイルの物理アドレス等を固有IDとしてコンピュータプログラムに埋め込み利用者コンピュータ2に提供する。このプログラムは、利用者コンピュータ2から固有IDを読み出し、埋め込まれた固有IDと一致したときに限って、プログラム本体を実行する。



(2)

特開2002-312052

1

【特許請求の範囲】

【請求項1】 コンピュータを特定して実行可能なコンピュータプログラムであって、コンピュータに固定された記憶媒体上の特定ファイルの物理アドレスを読み出し、この読み出した物理アドレスと予め当該コンピュータプログラムに設定された物理アドレスとが一致するか否かを判定し、一致すると判定された場合に当該コンピュータプログラムに予め設定された処理を実行することを特徴とするコンピュータプログラム。

【請求項2】 前記特定ファイルが読取専用ファイル、システムファイル、隠しファイルのいずれかの属性をもつファイルであることを特徴とする請求項1記載のコンピュータプログラム。

【請求項3】 実行されるコンピュータに固定された記憶媒体上の特定ファイルの物理アドレスを読み出し、この読み出した物理アドレスと予め設定された物理アドレスとが一致するときに予め設定された処理を実行するようにしたコンピュータを特定して実行可能なコンピュータプログラムの生成方法であって、入手された前記特定ファイルの物理アドレスを前記予め設定された物理アドレスとして前記コンピュータプログラムに設定することを特徴とするコンピュータプログラムの生成方法。

【請求項4】 コンピュータを特定して実行可能なコンピュータプログラムであって、コンピュータに設けられた通信部品の物理アドレスを読み出し、この読み出した物理アドレスと予め当該コンピュータプログラムに設定された物理アドレスとが一致するか否かを判定し、一致すると判定された場合に当該コンピュータプログラムに予め設定された処理を実行することを特徴とするコンピュータプログラム。

【請求項5】 実行されるコンピュータに設けられた通信部品の物理アドレスを読み出し、この読み出した物理アドレスと予め設定された物理アドレスとが一致するときに予め設定された処理を実行するようにしたコンピュータを特定して実行可能なコンピュータプログラムの生成方法であって、入手された前記通信部品の物理アドレスを前記予め設定された物理アドレスとして前記コンピュータプログラムに設定することを特徴とするコンピュータプログラムの生成方法。

【請求項6】 コンピュータを特定して実行可能なコンピュータプログラムの提供方法であって、コンピュータに固定された記憶媒体上の特定ファイルであって、読取専用ファイル、システムファイル、隠しファイルのいずれかの属性をもつファイルの物理アドレス

2

と、当該コンピュータに設けられた通信部品の物理アドレスとを通信回線を介して取得し、実行されるコンピュータに固定された記憶媒体上の特定ファイルの物理アドレスと、当該コンピュータに設けられた物理アドレスとを読み出し、当該読み出した各物理アドレスと予め設定された対応する各物理アドレスとが予め定められた一致条件を満たすときに予め設定された処理を実行するコンピュータプログラムに対し、前記取得した物理アドレスを前記予め設定された物理アドレスとして設定し、

この設定がなされたコンピュータプログラムを前記通信回線を介して前記コンピュータに提供することを特徴とするコンピュータプログラムの提供方法。

【請求項7】 予め前記コンピュータが利用する通信回線に対応する発信者番号通知により該コンピュータを認証することを特徴とする請求項6記載のコンピュータプログラムの提供方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、不正コピーを防止できるコンピュータプログラム、コンピュータプログラムの生成方法、コンピュータプログラムの提供方法に関する。

【0002】

【従来の技術】近年さまざまなビジネスのIT化に伴い、顧客へのサービスがコンピュータアプリケーションソフトウェアや電子データによって行われるようになってきた。また、従来からコンピュータのソフトウェアを製造・販売する事業もますます盛んになりつつあるが、一方そのソフトウェアプログラムや電子データはその性質上、コピーが簡単であり、また不正コピー利用防止については利用者に依存する部分が多く、インターネット接続環境の一般普及なども助力し、ネットワーク上で多くの不正コピーが流通するようになっている。

【0003】

【発明が解決しようとする課題】従来にあっては、不正コピーの防止方法がいくつか存在するが、これには以下の弱点・問題点が内在する。

【0004】従来にあっては、不正コピー防止のため

に、正規利用者へのみシリアルナンバーやキーワードなどの保護解除コードの配布をする。このため、別のコンピュータ、あるいは第3者への保護解除コードを教えると無限に不正利用されてしまう。また、配布するプログラムはネットワークやCD-R、CD-R/Wによる流通が容易であり、しかも大規模に行うことができる。

【0005】また、不正コピー防止のために、ネットワークを用いたプロダクトID（製品番号）をユーザ登録して監視することがある。このため、ネットワーク上で個人認証を行わない限り、正規利用者による登録なのか、不正コピーの登録なのか判別できない。（2重登録

(3)

特開2002-312052

3

を監視しても、それが正規利用者が再インストールをしたりPCを買い換えたりした場合と不正コピーの登録なのかは判別が不可能、通常は2重登録を許可している。)

また、不正コピー防止のために、コピーや解析が不可能なハードウェアキー(パラレルポート dongle やUSBキーなど)を正規利用者へのみ配布することがある。このため、ハードウェアキーのコストが大きいと、販売するソフトウェアプログラムが高価になってしまう。また、ハードウェアキーの故障や紛失についての対策にコストがかかる。(再発行でも実費がそれ以上の負担を正規利用者へ強いることになる。)

このような不正コピーにより、ソフトウェア業者は少なからぬ被害を被っており、また、安易に行える不正コピーによる消費者のモラル低下も懸念されている。

【0006】そこで本発明は、上記従来の事情に鑑みなされたものであり、その目的とするところは、により、プログラムの不正コピーが防止できるコンピュータプログラム、コンピュータプログラムの生成方法、コンピュータプログラムの提供方法を提供することにある。

【0007】

【課題を解決するための手段】上記従来の課題を解決するために、本発明の請求項1にあっては、コンピュータを特定して実行可能なコンピュータプログラムであって、コンピュータに固定された記憶媒体上の特定ファイルの物理アドレスを読み出し、この読み出した物理アドレスと予め当該コンピュータプログラムに設定された物理アドレスとが一致するか否かを判定し、一致すると判定された場合に当該コンピュータプログラムに予め設定された処理を実行することを特徴とするコンピュータプログラムをもって解決手段とする。

【0008】また、本発明の請求項2にあっては、前記特定ファイルが読取専用ファイル、システムファイル、隠しファイルのいずれかの属性をもつファイルであることを特徴とする請求項1記載のコンピュータプログラムをもって解決手段とする。

【0009】また、本発明の請求項3にあっては、実行されるコンピュータに固定された記憶媒体上の特定ファイルの物理アドレスを読み出し、この読み出した物理アドレスと予め設定された物理アドレスとが一致するときに予め設定された処理を実行するようにしたコンピュータを特定して実行可能なコンピュータプログラムの生成方法であって、入手された前記特定ファイルの物理アドレスを前記予め設定された物理アドレスとして前記コンピュータプログラムに設定することを特徴とするコンピュータプログラムの生成方法をもって解決手段とする。

【0010】また、本発明の請求項4にあっては、コンピュータを特定して実行可能なコンピュータプログラムであって、コンピュータに設けられた通信部品の物理アドレスを読み出し、この読み出した物理アドレスと予め

4

当該コンピュータプログラムに設定された物理アドレスとが一致するか否かを判定し、一致すると判定された場合に当該コンピュータプログラムに予め設定された処理を実行することを特徴とするコンピュータプログラムをもって解決手段とする。

【0011】また、本発明の請求項5にあっては、実行されるコンピュータに設けられた通信部品の物理アドレスを読み出し、この読み出した物理アドレスと予め設定された物理アドレスとが一致するときに予め設定された処理を実行するようにしたコンピュータを特定して実行可能なコンピュータプログラムの生成方法であって、入手された前記通信部品の物理アドレスを前記予め設定された物理アドレスとして前記コンピュータプログラムに設定することを特徴とするコンピュータプログラムの生成方法をもって解決手段とする。

【0012】また、本発明の請求項6にあっては、コンピュータを特定して実行可能なコンピュータプログラムの提供方法であって、コンピュータに固定された記憶媒体上の特定ファイルであって、読取専用ファイル、システムファイル、隠しファイルのいずれかの属性をもつファイルの物理アドレスと、当該コンピュータに設けられた通信部品の物理アドレスとを通信回線を介して取得し、実行されるコンピュータに固定された記憶媒体上の特定ファイルの物理アドレスと、当該コンピュータに設けられた物理アドレスとを読み出し、当該読み出した各物理アドレスと予め設定された対応する各物理アドレスとが予め定められた一致条件を満たすときに予め設定された処理を実行するコンピュータプログラムに対し、前記取得した物理アドレスを前記予め設定された物理アドレスとして設定し、この設定がなされたコンピュータプログラムを前記通信回線を介して前記コンピュータに提供することを特徴とするコンピュータプログラムの提供方法をもって解決手段とする。

【0013】また、本発明の請求項7にあっては、予め前記コンピュータが利用する通信回線に対応する発信者番号通知により該コンピュータを認証することを特徴とすることを特徴とする請求項6記載のコンピュータプログラムの提供方法をもって解決手段とする。

【0014】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。図1は、本発明の一実施の形態に係るネットワークインストールシステムの構成図である。

【0015】このシステムにあっては、プログラムを特定のコンピュータ(実施の形態では利用者コンピュータ2という)に限って利用できるようにするために、ネットワークインストールサーバ1が、利用者コンピュータ2に固有の識別情報(固有IDまたはコンピュータ固有IDという)を、利用者コンピュータ2に配布されるプログラムに設定し(プログラム本体に付与し)、ネッ

50

(4)

特開2002-312052

5

トワークを介して利用者コンピュータ2へ配布（送信）する。

【0016】そして、利用者コンピュータ2では、当該プログラムが、利用者コンピュータ2から固有IDを読み出し、この固有IDと自身に埋め込まれた固有IDとが、一致条件を満たせば、プログラム本体の処理を実行するようになっている。

【0017】なお、利用者コンピュータ2は、コンピュータのみならず、コンピュータの機能を備える装置、例えば、携帯電話やPHS端末、ホームゲートウェイ装置、インターネット家電を含むものとして位置づける。

【0018】本実施の形態では、固有IDとして、ハードディスク上における特定ファイルの物理的位置情報とLANカードのMACアドレスを用いている。

【0019】ここで、ネットワークインストールサーバ1や利用者コンピュータ2を説明する前に、発明の概略とベースとなる技術を説明する。

【0020】コンピュータを特定するということは、認証ができるということにもなる。ネットワーク上の認証ということについては、これまで主にユーザ認証について論じられてきた。ただし、このユーザという概念は、必ずしも現実世界に存在する人物の特定というわけにはいかない。つまり、本当のところ誰だかわからないのである。したがって、物品の收受や金銭のやり取りのような現実世界の行為を適用しようとする、「ユーザ」を「（実存する）カード番号」に置き換える等することによって、常に現実世界との結びつきを別途行わなければならない。本発明のコンピュータとは物理的な「モノ」であり、現実世界に存在する「モノ」と「ユーザ」の結びつきを作ることができる。インターネット上で提供されるサービスではインターネット上で完結しているものと、現実世界と結合しているものがある。本発明は後者のサービスにおいて有効な解決手段のひとつとなり得るものである。

【0021】図2は、ハードディスクの物理的なデータ格納方法を示す図である。図3は、物理アドレスを示す図である。

【0022】例えば、ファイル「alpha」がハードディスクに格納される手順は以下の通りである。手順①「alpha」の大きさを調べ、格納できるかどうかを確認する。手順②ハードディスク上の空きクラスタを集める。手順③「alpha」を最小クラスタサイズに分割する。手順④各クラスタの位置へ「alpha」を格納する。手順⑤「alpha」のデータ要素を持っている各クラスタの位置情報をファイル名alphaをマッピングしてデータテーブルに格納する。

【0023】上記手順の②において、あるファイルにどのクラスタが割り当てられるかについてはコンピュータの使用状況、つまり空き領域が記録媒体上のどこにあるか、それぞれのコンピュータで異なる。これはコンピュ

6

ータがハードディスクを空いている領域から順番に効率よく使用するからである。例えばデータの中身も内容も同じファイル「beta」を2台のコンピュータの同じディレクトリ位置（論理的な位置）に格納しても、ハードディスク上の物理的な位置は必ずしも同じにはならないのである。同じになる確率はハードディスクの容量が大きければ大きいほど低くなる。例えば20GBのハードディスクを2KBのクラスタブロックで使用している場合、同じ物理的位置に格納される確率は、 $2KB/20GB = 2000/200000000000 = 1/1000$ 万分の1となる。厳密には更にクラスタサイズが何KBであるか、サイズ固定であるか可変であるかによって、さらに確率は低くなる。もので、ハードディスクは取り外し交換等が困難であるため、コンピュータの特定が確実に行える。

【0024】ハードディスク上では空き領域を格納するファイルのサイズ分の空き領域を集めてくる。この空き領域はクラスタサイズというサイズに区画されており、最終的にファイルが格納できる数の区画を用意する。一つのファイル格納のために使用される区画はディスク上で連続しているわけではなく、離散している。ハードディスクは領域を効率よく使用するためにディスクの内側から空いている区画を拾い出して用意するため、内側に近い場所で空いている領域があればそこから割り当てる。

【0025】ここで、あるファイルの物理アドレスをコンピュータ固有のIDとして配布プログラムに埋め込み、動作時に比較することで、そのコンピュータだけで動作するプログラムが可能になるのである。

【0026】それぞれのプログラムはあるコンピュータの固有ID（あるファイルのハードディスク物理格納位置情報）を持っており、プログラムの動作を（1）あるファイル（この例では「alpha」）の物理アドレスを調べる。（2）自分自身に埋め込まれている固有IDと比較する。（3）合致するならば本来動作、合致しなければ動作終了する。

【0027】こうすることで、このプログラムはある特定のコンピュータ（対価の支払いをしたなどのそのプログラムおよびサービスを受ける資格や権利があるコンピュータ）以外のコンピュータでは動作しないため、不正にコピーして使用することができなくなる。

【0028】ここで、ハードディスク物理格納位置情報（物理アドレス）を詳しく説明する。

【0029】図3に示すように、ハードディスク上のあるファイルのアドレス（シリンダNo：ヘッドNo：セクタNoもしくはクラスタブロックアドレス）は、以下のようになる。

【0030】ファイルデータはOS（オペレーティングシステム）のファイルシステムによって割り当てられたクラスタブロックの単位に分割されて保存される。クラ

10

20

30

40

50

(5)

特開2002-312052

7

スタブブロックは、ディスク上の物理的な最小単位（セクタ）のまとまりで構成されている。したがって、ファイルの入出力はファイル名（ファイルシステム上の位置）→クラスタブロック位置→物理構造上の位置（シリンダNo:ヘッドNo:セクタNo）で管理されているあるファイルの物理構造上の位置やクラスタブロック位置はコンピュータのハードディスクのサイズやオペレーションシステムによって異なる。また、新たに追加されたファイルへのディスク領域の割り当ては、空き領域から割り当てられるため、同じハードウェア構成のコンピュータであっても使用している期間や、使用方法によって割り当てられる物理構造上の位置は異なるのである。ただし、そのディスク上のアドレスは唯一無二ではない。仮に20GBのハードディスクを持つ2台のコンピュータがあるとすれば、あるファイルに同じディスク上のアドレスが割り当てられる確率は、クラスタサイズが2KBの場合、1000万分の1の確率である。今後のハードディスク容量の増加傾向を考えると、ソフトウェア配布を目的としたコンピュータ特定には十分な数値である。ただし、実際の運用時には故障時などを想定し、次のMACアドレスをコンピュータ固有のIDに付加し、OR条件で利用することで、さらなる利便性が確保される。

【0031】ここで、Ethernetカード（LANカード、NIC: Network Interface Cardともいう）のMACアドレスについて説明する。

【0032】EthernetカードのMACアドレスは、6バイトのコードで、先頭3バイトがベンダーコード、残り3バイトがベンダー内で重複しないよう管理しているコードであるため、世界中で唯一無二のコードである。（コードパターンは281兆4749億7671万0656通り）抜き差しがある程度自由なものもあるため、実運用時にはハードディスクの故障やコンピュータの買い替えなどを想定し、OR条件で併用することで、コンピュータの特定をサポートすることができる。

【0033】次に、図4を参照して、クラスタブロックの不確定性に関し説明する。

【0034】ファイルデータはOSのファイルシステムによって割り当てられたクラスタブロックの単位に分割されて保存されている。データの読み出しはそのデータを構成するクラスタをすべて集め、つなぎ合わせ、データの書き込みはファイルをクラスタ単位に分割する。

【0035】ディスク領域はこのクラスタ単位で分割されており、新たにファイルの書き込みが発生した場合は、空いている領域から割り当てられるため、データ消去、書き込みなどを繰り返すうちに、フラグメンテーション（クラスタブロックの不連続）が発生する。フラグメンテーションが多く発生すると、当然ディスクI/Oのパフォーマンスが低下するが、それを解消するために、データをつなぎ合わせて、アタマから順番に一続き

8

ずつ書き込むようにするソフトウェアとして、いわゆるデフラグツールがある。デフラグツールによって、ファイルのディスク上のアドレスは変動するため、流動的で不確定となってしまう場合が考えられる。

【0036】しかしそのデフラグツールのほとんどが、移動させるファイルの属性を見て、「隠しファイル」「システムファイル」「読取専用ファイル」であれば例外的にファイルの移動をしない。そのため、それらのファイルのディスク上のアドレスは、ディスクをフォーマットしたり、OSを再インストールしない限り変わらない。しかもそのアドレスはコンピュータ毎に異なるものとなる。したがって、あるファイルに隠しファイル・システムファイル・読取専用の属性を与え、さらにそのファイルが格納されたアドレスをファイルに書いておけば、格納位置のアドレスと比較することによってそのファイルがコピーされたか否かを検知できる。

【0037】次に、ハッシュ値について説明する。

【0038】ハッシュ値は、ハッシュ関数と呼ばれる1方向の関数によって得られる値、ハッシュ関数一方向であり、得られた値から元の値へ戻すことはできない。

（ため、見ても意味がわからない）アルゴリズムにはMD5、SHA-1などがある。例えばMACアドレス00:00:E2:11:C6:C1をアルゴリズムSHA-1のハッシュ関数にかけると E2C94DA022471F7E813F325FF2D949D1（大きさ 128Bytes）になり、アルゴリズムMD5のハッシュ関数にかけると、5BD90EEC626DDFDE60852F1A3EAC9BE3177E7963（大きさ 160Bytes）になる。

【0039】例えば、ディスクセクタアドレス0255CYL-000HED-01SECをアルゴリズムSHA-1のハッシュ関数にかけると11170A738232655D72F268E0088B3CFF（大きさ 128Bytes）となり、アルゴリズムMD5のハッシュ関数にかけると、34C72089A99B85034E21A04B9B94DF700E533735（大きさ 160Bytes）となる。

【0040】ハッシュ値の元の値はコンピュータ固有のものであり、ハッシュ値はプログラムをインストールするコンピュータ毎に違う値となる。異なるコンピュータでインストールして、プログラムをコピーしても、このハッシュ値が異なるため、インストーラB'、プログラム本体は動作しない。またハッシュ値を生成しようとしても、元の値がなにかはハッシュ値をみてもわからない。

【0041】従って、ハッシュ値を解析しても、固有IDを知ることは殆ど不可能となる。図5は、ネットワークを介したインストール管理のシーケンス図である。図6は、顧客DB11に設定されたネットワークインストールの運用条件を示す図である。

(6)

特開2002-312052

9

【0042】ネットワークインストールサーバ1は、顧客に関するデータを格納するための顧客DB11と、利用者コンピュータ2へ提供するプログラムの本体であるプログラム本体を格納したプログラムDB12とを備える。これらDB11、12はハードディスク等の記憶装置内の記憶領域に構成される。

【0043】また、プログラム本体に固有IDを埋め込む等の処理を行うプログラム生成部13を備え、利用者コンピュータ2とプログラム等を交信できるようになっている。プログラム生成部13はプログラム生成のために予めネットワークインストールサーバ1に記憶された処理プログラムを実行することで実現される。

【0044】利用者コンピュータ2は、ネットワークインストールサーバ1を利用するために最適化されたプログラムであるネットワークインストーラ21を備える。ネットワークインストーラ21は、プログラムIDや顧客IDが入力され、所定の操作がなされると、これをネットワークインストールサーバ1へ送信して、プログラムを要求するといった動作を行うようになっている次に、本実施の形態の動作を説明する。

【0045】図6に示すように、種々の許可を下すための条件が顧客DB11に設定される。顧客DB11における顧客が利用するプログラム毎のデータ列、具体的には、当該顧客の顧客IDと、当該顧客が購入したプログラムのプログラムIDと、購入済みであることを示す「購入」とが設定されたデータ列に、適宜ステータス、コンピュータ固有ID（MACアドレス）、コンピュータ固有ID（ハードディスクのファイルアドレス）がそれぞれ設定される。

【0046】インストールを許可するためには、ステータス、コンピュータ固有ID（MACアドレス）、コンピュータ固有ID（ハードディスクのファイルアドレス）はそれぞれ、値が未設定である必要がある。かかる値がインストール許可条件である。

【0047】アンインストールを許可するには、ステータスは「インストール」、コンピュータ固有ID（MACアドレス）、コンピュータ固有ID（ハードディスクのファイルアドレス）のそれぞれに、当該顧客のコンピュータから送信されたMACアドレス、ハードディスクのファイルアドレスが設定されている必要がある。かかる値がアンインストール許可条件である。

【0048】なお、ユーザが使用するコンピュータを替えるための、再インストールを許可するには、設定された顧客IDと送信された顧客IDとが一致する必要がある。また、ハードディスクの故障時やアンインストール失敗時を想定し、顧客IDまたはプログラムIDのどちらかが、利用者コンピュータ2から送信されたものと一致することを条件としてもよい。

【0049】図5に示すように、ネットワークインストールサーバ1では、プログラムを購入した顧客の電話番

10

号等の顧客情報から、事前に認証用の顧客IDを生成し、その顧客が購入したプログラムのプログラムIDを関連づけて顧客DB11へ格納しておく。

【0050】一方、ネットワークインストールサーバ1からの指令に応じて、利用者コンピュータ2でのプログラムのインストール等を制御するネットワークインストーラ21が配布され、利用者コンピュータ2に事前にインストールされる。

【0051】図5に示すように、ネットワークインストーラ21には、インストールしたいプログラムのプログラムIDと顧客IDとを登録しておく。

【0052】先ずネットワークインストーラ21は、利用者コンピュータ2内を走査し、特定のファイル（読取専用・システム・隠しファイル属性をもつもの）に限る。これ以降、「ファイルF1」と呼ぶ）のハードディスク上のアドレスを固有IDとして取得する。また、ネットワークインストーラ21は、利用者コンピュータ2を走査し、LANカードのMACアドレスを固有IDとして取得する。そして、顧客IDとプログラムIDと2つの固有IDとインストール要求とをネットワークインストールサーバ1に送信する（ステップS1）。

【0053】これに対しネットワークインストールサーバ1は、顧客IDとプログラムIDを顧客DB11に格納されたインストール許可条件を参照してインストールの資格があるかどうか確認する。利用資格がある場合は、ネットワークインストールサーバ1は、送信されたプログラムIDを付与されたプログラム（プログラムAとする）をプログラムDB12から読み出し、これに対し、送信された固有IDのハッシュ値を動作制限識別情報として埋め込んでプログラムA-1を生成し、利用者コンピュータ2へ送信する（ステップS3）。

【0054】送信されたプログラムA-1は利用者コンピュータ2に格納され、ネットワークインストーラ21により自動的に起動される。起動されたプログラムA-1は、利用者コンピュータ2内の固有IDとプログラムA-1に埋め込まれた固有IDとが一致するかを判定し、一致していれば、インストールが完了した旨をネットワークインストールサーバ1に通知する（ステップS5）。なお、ファイルF1の物理アドレス同士が一致し、かつMACアドレス同士が一致する場合に「一致する」という判定結果としても良いし、どちらかが一致する場合に「一致する」という判定結果としても良い。なお、以下においても同様に、適宜判定基準を定め、この判定基準により判定することができる。

【0055】通知を受けたネットワークインストールサーバ1は、この完了通知を顧客DB11及びプログラムDB12に反映する。つまり、ステータスを「インストール」に設定し、ハードディスクのファイルF1の物理アドレスとMACアドレスを設定する。そして、出荷本数をカウントする処理を行う。

50

(7)

特開2002-312052

11

【0056】一方、利用者コンピュータ2においては、プログラムA-1に含まれる本体プログラムAが、本来実行すべき処理を行う。

【0057】ここで、上記インストール管理のシーケンスにおけるプログラムの動作をフローチャートを参照して説明する。

【0058】図7は、固有IDの送信時の処理の流れを示すフローチャート図である。

【0059】ネットワークインストーラ21に顧客IDとダウンロードしたいプログラムのプログラムIDを入力すると（ステップS101）、ネットワークインストーラ21はまず、利用者コンピュータ2を走査し、ファイルF1のハードディスク上のアドレス、つまり固有IDを取得する（ステップS103）。次に、利用者コンピュータ2を走査し、NIC（LANカード）のMACアドレス（固有ID）を取得する（ステップS105）。次に、これら固有IDをネットワークインストールサーバ1に送信する（ステップS107）。

【0060】これに対しネットワークインストールサーバ1は、顧客IDとプログラムIDを顧客DB11内で検索し、利用資格があるかどうか確認し、利用資格がある場合は、固有IDを顧客DB11に格納する（ステップS109）。

【0061】図8は、ネットワーク配布の際の処理の流れを示すフローチャート図である。まず、プログラム生成部13は、送信されてきた固有IDをハッシュ関数にかける（ステップS111）。次に、得られたハッシュ値をプログラムAに格納してプログラムA-1を生成する（ステップS113）。そして、生成したプログラムA-1を利用者コンピュータ2へ送信する（ステップS115）。

【0062】図9は、配布後の処理の流れを示すフローチャート図である。ネットワークインストールサーバ1から送信されたネットワークインストーラ21はまず、コンピュータを走査して固有IDを取得し、ハッシュ関数にかける（ステップS121）。次に、得られたハッシュ値とネットワークインストールサーバ1で埋め込まれたハッシュ値と比較する（ステップS123）。ここで、不一致のときは、エラーを出力して動作を終了する（ステップS125）。一方、一致のときは、プログラム本体を抽出して動作させる（ステップS127）。

【0063】図10は、完了通知の送信時の処理の流れを示すフローチャート図である。プログラムが正規利用者へ配布された場合にネットワークインストーラ21は、顧客ID、コンピュータ固有ID、プログラムIDをネットワークインストールサーバ1へ送信する（ステップS131）。ネットワークインストールサーバ1は、各DBへIDを登録し、インストール状況フラグを変更する（ステップS133）。

【0064】次に、ネットワークを介したアンインスト

12

ール管理を説明する。図11は、ネットワークを介したアンインストール管理のシーケンス図である。図11に示すように、ネットワークインストールサーバ1では、プログラムを購入した顧客の固有IDとインストールされているプログラムのプログラムIDを顧客DB11に事前に登録しておく。

【0065】ネットワークインストーラ21がアンインストールオプションで起動されると、利用者コンピュータ2内を走査して固有IDを取得する。そして、ネットワークインストーラ21は、顧客IDとプログラムIDと固有IDとアンインストール要求をネットワークインストールサーバ1に送信する（ステップS11）。

【0066】これに対しネットワークインストールサーバ1は、顧客DB11のアンインストール許可条件を参照して、アンインストールの資格があるかどうか確認する。資格がある場合は、アンインストールコマンドを発行、送信する（ステップS13）。

【0067】ネットワークインストーラ21は、アンインストールを開始し、これが正常に終了したらアンインストール完了通知をネットワークインストールサーバ1に送信する（ステップS15）。

【0068】通知を受けたネットワークインストールサーバ1は、この完了通知を顧客DB11及びプログラムDB12に反映する。すなわち、顧客DB11の該当するステータスを「アンインストール」に設定する。

【0069】次に、発信者番号認証によるアクセスコントロールを付加したときのインストール管理を説明する。図12は、発信者番号認証によるアクセスコントロールを付加したときのインストール管理のシーケンス図である。図12に示すように、プログラムを購入した顧客の電話番号をフレッツオフィス網（都道府県毎に設けられたIP網、「地域IP網」と顧客DBへ事前に登録し、さらに電話番号等の顧客情報と認証用ユーザ名を関連づけて顧客DB11に格納しておく。

【0070】一方、ネットワークインストーラ21には、インストールしたいプログラムのプログラムIDを登録しておく。

【0071】まず、利用者コンピュータ2が利用する電話回線の番号（発信者番号）が地域IP網のリモートアクセスサーバ（RAS）に送信され（ステップS21）、RAS内で発信者の認証が行われる。すなわち、登録した電話番号からのみ接続が許可される。なお、かかる通知を発信者番号通知という。

【0072】接続が許可されると、ネットワークインストーラ21がユーザ名とパスワードをネットワークインストールサーバ1に送信し（ステップS23）、ネットワークインストールサーバ1がこれに回答する（ステップS25）。これ以降は、図5に示した処理と同様の処理が行われる。

【0073】なお、発信者番号認証によるアクセスコン

10

20

30

40

50

(8)

特開2002-312052

13

トロールを付加したときのアンインストール管理については、図13の発信者番号認証によるアクセスコントロールを付加したときのアンインストール管理のシーケンス図に示すように、図12に示した処理と同様の発信者認証および応答が行われ、その後、図11に示した処理と同様のアンインストール管理が行われる。

【0074】本実施の形態では、このように、コンピュータ固有IDによりプログラムの不正コピーが防止される。また、アンインストール管理を行っているため、重複インストールはできない。つまり、アンインストールしなければインストールするためのプログラムは送信されない。

【0075】なお、上記説明した処理を実行する処理プログラムは、半導体メモリ、磁気ディスク、光ディスク、光磁気ディスク、磁気テープなどのコンピュータ読み取り可能な記録媒体に記録して、この記録媒体をコンピュータシステムに組み込むとともに、この記録媒体に記録されたプログラムをコンピュータシステムにダウンロードまたはインストールし、このプログラムでコンピュータシステムを作動させることにより、プログラム生成方法を実施するプログラム生成装置として機能させることができるのは勿論であり、このような記録媒体を用いることにより、その流通性を高めることができる。

【0076】また、上記実施の形態では、利用者コンピュータ2を特定する手段としてファイルF1の物理アドレスやLANカードの物理アドレスを利用したが、これらに代えて、CPUのシリアルナンバーや、ICカードや指紋認証デバイス等のハードウェアの識別情報を利用することができる。

【0077】以上説明したように、本実施の形態によれば、利用者コンピュータ2を特定して実行可能なプログラムA-1は、利用者コンピュータ2に固定された記憶媒体、つまりハードディスク上の特定ファイルF1の物理アドレスや利用者コンピュータ2に設けられた通信部品であるLANカードの物理アドレスを読み出し、この読み出した物理アドレスと予めプログラムA-1に設定された物理アドレスとが一致するか否かを判定し、一致すると判定された場合にプログラムA-1に予め設定されたプログラム本体の処理を実行するので、このプログラムA-1は、他のコンピュータでは動作せず、従って、プログラムの不正コピーを防止できる。

【0078】また、特定ファイルが読取専用ファイル、システムファイル、隠しファイルのいずれかの属性をもつファイルであるので、フラグメンテーションが発生したときでも変わらない物理アドレスにより、プログラムの不正コピーを一層確実に防止できる。

【0079】また、利用者コンピュータ2に固定された記憶媒体上のファイルF1の物理アドレスや利用者コンピュータ2に設けられた通信部品の物理アドレスを読み出し、この読み出した物理アドレスと予め設定された物

14

理アドレスとが一致するときに予め設定された処理を実行するようにしたプログラムA-1を生成する際に、入手された前記特定ファイルの物理アドレスを前記予め設定された物理アドレスとしてこのプログラムA-1に設定するので、他のコンピュータでは動作せず、従って、プログラムの不正コピーを防止できるコンピュータプログラムを生成することができる。

【0080】また、利用者コンピュータ2を特定して実行可能なコンピュータプログラムA-1の提供に際して、利用者コンピュータ2に固定された記憶媒体上の特定ファイルであって、読取専用ファイル、システムファイル、隠しファイルのいずれかの属性をもつファイルF1の物理アドレスと、利用者コンピュータ2に設けられた通信部品の物理アドレスとを通信回線を介して取得し、実行されるコンピュータに固定された記憶媒体上の特定ファイルの物理アドレスと、当該コンピュータに設けられた物理アドレスとを読み出し、当該読み出した各物理アドレスと予め設定された対応する各物理アドレスとが予め定められた一致条件を満たすときに予め設定された処理を実行するコンピュータプログラムに対し、前記取得した物理アドレスを前記予め設定された物理アドレスとして設定し、この設定がなされたコンピュータプログラムを前記通信回線を介して前記コンピュータに提供するコンピュータプログラムの提供方法をネットワークインストールサーバ1が実施するので、かかる方法によっても、プログラムの不正コピーを防止できる。

【0081】また、地域IP網のRASが、予め利用者コンピュータ2が利用する通信回線に対応する発信者番号通知により該コンピュータを認証するので、かかる方法によっても、プログラムの不正コピーをより確実に防止できる。また、発信者番号によって顧客が特定できるので、料金後払いによるプログラムの販売を行えるという付帯効果も得られる。

【0082】

【発明の効果】以上説明したように、本発明によれば、コンピュータに固定された記憶媒体上の特定ファイルの物理アドレスや、コンピュータに設けられた通信部品の物理アドレスを読み出し、この読み出した物理アドレスと予め当該コンピュータプログラムに設定された物理アドレスとが一致するか否かを判定し、一致すると判定された場合に当該コンピュータプログラムに予め設定された処理を実行するようにしたので、このプログラムを他のコンピュータで実行することができず、従って、プログラムの不正コピーを防止できる。

【0083】また、本発明によれば、実行されるコンピュータに固定された記憶媒体上の特定ファイルの物理アドレスや、コンピュータに設けられた通信部品の物理アドレスを読み出し、この読み出した物理アドレスと予め設定された物理アドレスとが一致するときに予め設定された処理を実行するようにしたコンピュータプログラムの生成に際

10

20

30

40

50

(9)

特開2002-312052

15

し、入手された前記特定ファイルの物理アドレスを前記予め設定された物理アドレスとして前記コンピュータプログラムに設定するようにしたので、このプログラムを他のコンピュータで実行することができず、従って、プログラムの不正コピーを防止できる。

【図面の簡単な説明】

【図1】本発明の一実施の形態に係るネットワークインストールシステムの構成図である。

【図2】ハードディスクの物理的なデータ格納方法を示す図である。

【図3】物理アドレスを示す図である。

【図4】クラスタブロックの不確定性に関する説明図である。

【図5】ネットワークを介したインストール管理のシーケンス図である。

【図6】顧客DB11に設定された運用条件を示す図である。

【図7】固有IDの送信時の処理の流れを示すフローチャート図である。

【図8】ネットワーク配布時の処理の流れを示すフロー

*チャート図である。

【図9】配布後の処理の流れを示すフローチャート図である。

【図10】完了通知の送信時の処理の流れを示すフローチャート図である。

【図11】ネットワークを介したアンインストール管理のシーケンス図である。

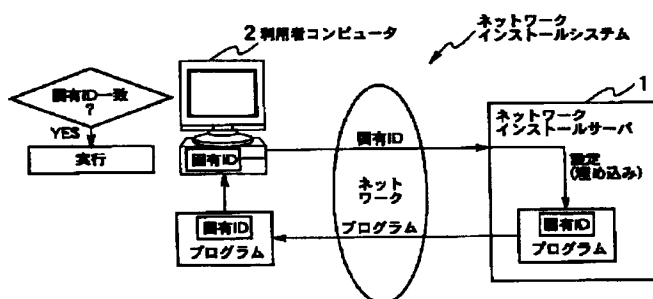
【図12】発信者番号認証によるアクセスコントロールを付加したときのインストール管理のシーケンス図である。

【図13】発信者番号認証によるアクセスコントロールを付加したときのアンインストール管理のシーケンス図である。

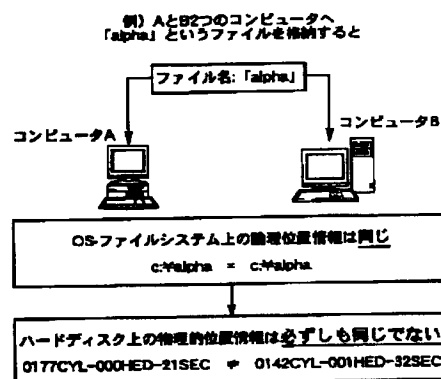
【符号の説明】

- 1 ネットワークインストールサーバ
- 2 利用者コンピュータ
- 11 顧客DB
- 12 プログラムDB
- 13 プログラム生成部
- 21 ネットワークインストーラ

【図1】



【図2】



【図4】

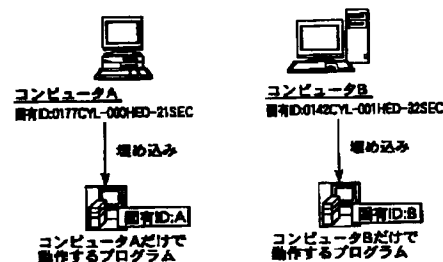
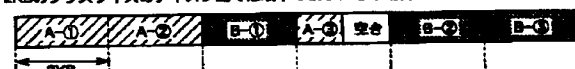
コンピュータ上で固有のIDについて

≒デフラグ等によるクラスタブロックの不確定性

ファイルA、ファイルBというデータが、



2KBのクラスサイズのディスク上では以下になる場合がある



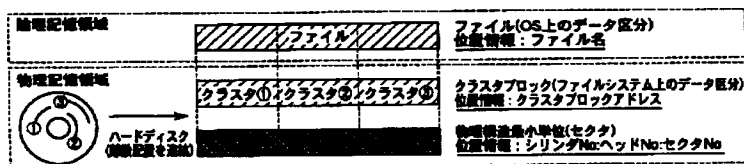
(10)

特開2002-312052

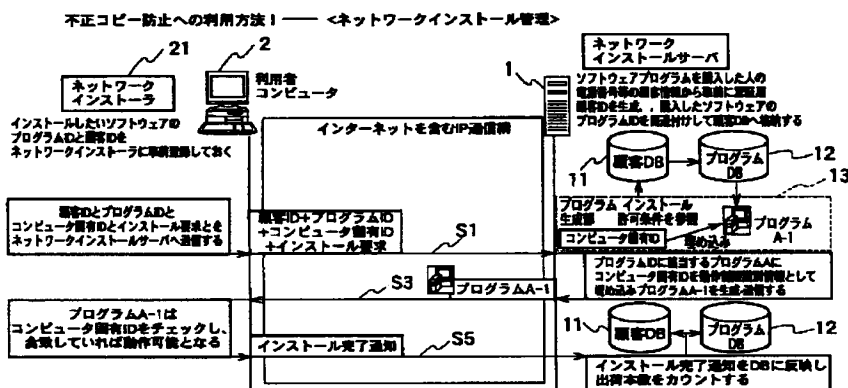
【図3】

コンピュータ上で固有のIDについて

■ハードディスク上のあるファイルの物理アドレス(シリンダNo:ヘッドNo:セクタNoもしくはクラスタブロックアドレス)



【図5】



【図6】

ネットワークインストール運用条件について

インストール許可条件

顧客ID	プログラムID	初期条件	ステータス	コンピュータ固有ID (MACアドレス)	コンピュータ固有ID (ハードディスク)
0001	A001	購入	-	NULL	NULL

アンインストール許可条件

※顧客IDとコンピュータID両方とも合致すればアンインストール可

顧客ID	プログラムID	初期条件	ステータス	コンピュータ固有ID (MACアドレス)	コンピュータ固有ID (ハードディスク)
0001	A001	購入	インストール	00:00:E2:11:C8:C1	0055C7L-000HED-01SEC

再インストール許可条件(重複インストール防止)

※顧客IDが両方とも合致すれば再インストール可(ただしステータスはアンインストール)

顧客ID	プログラムID	初期条件	ステータス	コンピュータ固有ID (MACアドレス)	コンピュータ固有ID (ハードディスク)
0001	A001	購入	アンインストール	00:00:E2:11:C8:C1	0055C7L-000HED-01SEC

→他のコンピュータへの切り替えが可能

※顧客IDとコンピュータ固有IDのどちらかが合致すれば再インストール可
(ハードディスク故障時やアンインストール失敗時など)

顧客ID	プログラムID	初期条件	ステータス	コンピュータ固有ID (MACアドレス)	コンピュータ固有ID (ハードディスク)
0001	A001	購入	インストール	00:00:E2:11:C8:C1	0055C7L-000HED-01SEC

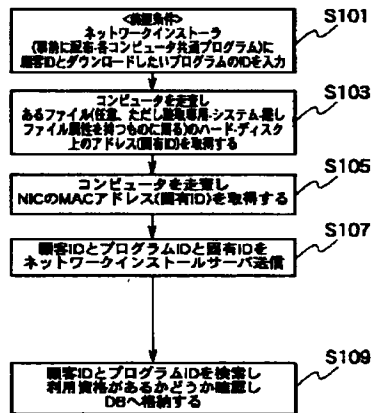
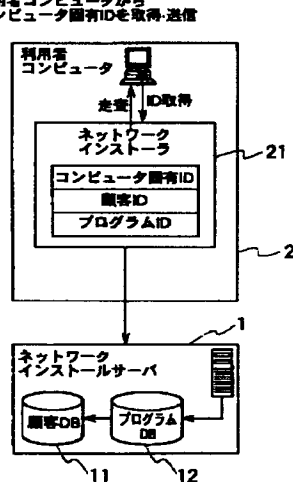
→再インストール後はハードディスクIDを書き換え

(11)

特開2002-312052

【図7】

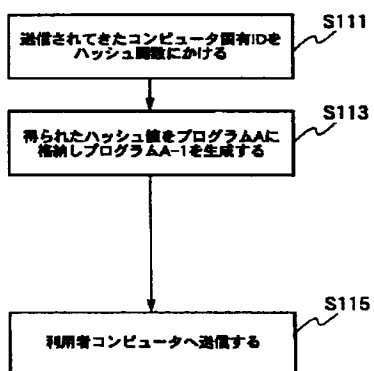
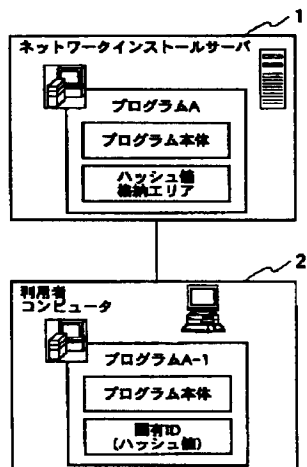
各プログラムの動作 固有IDの送信

利用者コンピュータから
コンピュータ固有IDを取得・送信

【図8】

各プログラムの動作 ネットワーク配布

あるコンピュータでのみ動作するプログラムの生成

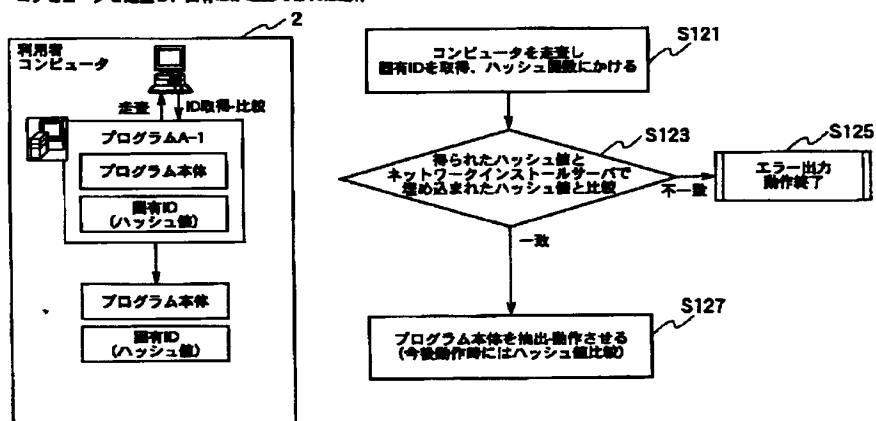


(12)

特開2002-312052

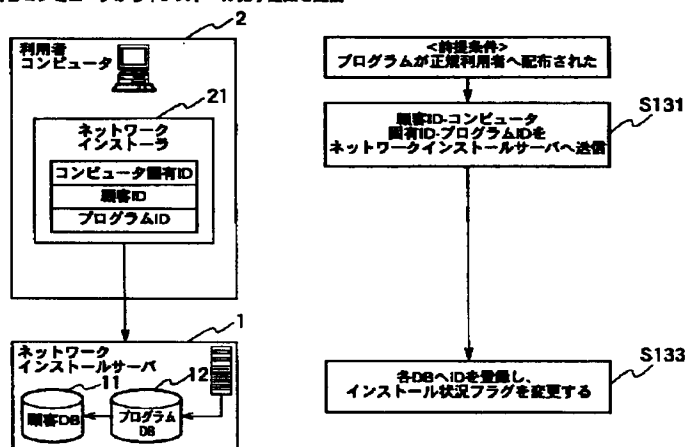
【図9】

各プログラムの動作 配布後の処理
コンピュータを走査し、固有IDが検出できれば動作



【図10】

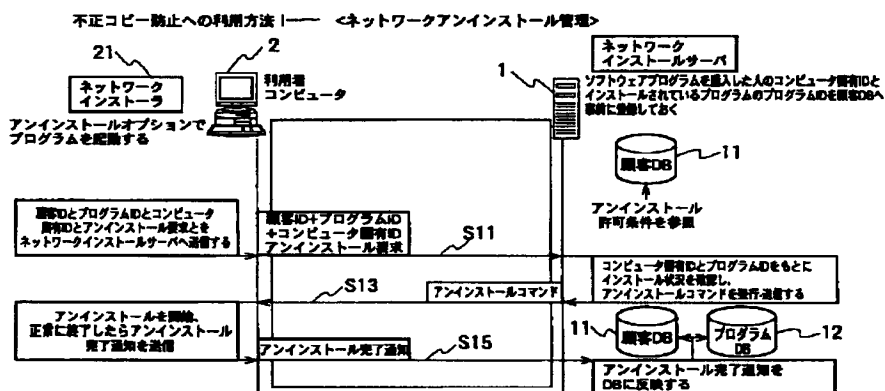
各プログラムの動作 完了通知の送信
利用者コンピュータからインストール完了通知を送信



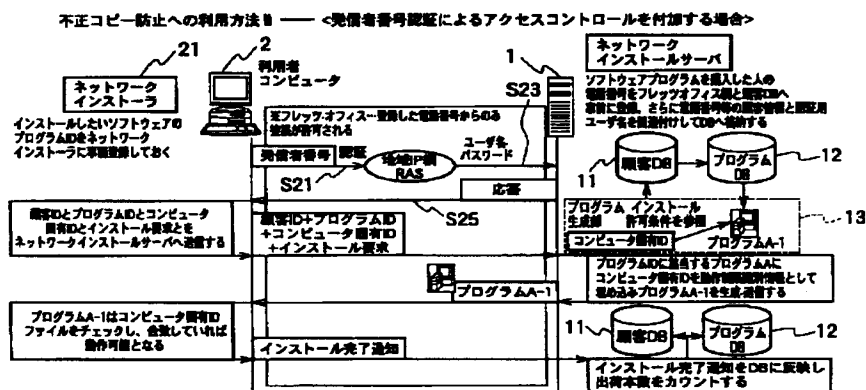
(13)

特開2002-312052

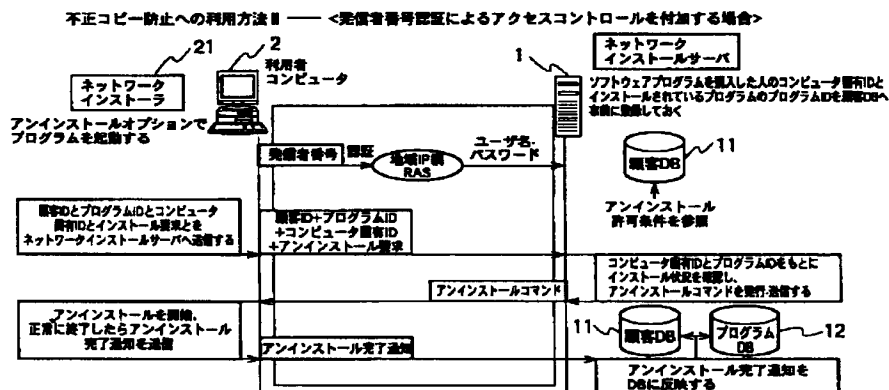
【図11】



【図12】



【図13】



(14)

特開2002-312052

フロントページの続き

(72)発明者 齊川 清二
大阪府大阪市中央区馬場町3番15号 西日
本電信電話株式会社内
(72)発明者 徳佐 幸展
大阪府大阪市中央区馬場町3番15号 西日
本電信電話株式会社内
(72)発明者 井ノ上 悦司
大阪府大阪市中央区馬場町3番15号 西日
本電信電話株式会社内

(72)発明者 水本 照彰
大阪府大阪市中央区馬場町3番15号 西日
本電信電話株式会社内
(72)発明者 渡辺 修一郎
大阪府大阪市中央区馬場町3番15号 西日
本電信電話株式会社内
(72)発明者 上野 真由美
大阪府大阪市中央区馬場町3番15号 西日
本電信電話株式会社内
Fターム(参考) 5B017 AA03 AA06 BA01 CA15
5B076 FB06